Domain 4 Cloud Application Security

Review Questions

**1.** Which of the following best represents the definition of REST?

**A.** Built on protocol standards

**B.** Lightweight and scalable

**C.** Relies heavily on XML

**D.** Only supports XML output

**2.** Which of the following is not one of the SDLC phases?

**A.** Define

**B.** Reject

**C.** Design

**D.** Test

**3.** Which of the following is *not* a component of the of the STRIDE model?

**A.** Spoofing

**B.** Repudiation

**C.** Information disclosure

**D.** External pen testing

**4.** Which of the following best describes SAST?

**A.** A set of technologies that analyze application source code, and bit code for coding and

design problems that would indicate a security problem or vulnerability

**B.** A set of technologies that analyze application bit code, and binaries for coding and

design problems that would indicate a security problem or vulnerability

**C.** A set of technologies that analyze application source code, byte code, and binaries for

coding and design problems that would indicate a security problem or vulnerability

**D.** A set of technologies that analyze application source code for coding and design problems that would indicate a security problem or vulnerability

**5.** Which of the following best describes data masking?

**A.** A method where the last few numbers in a dataset are not obscured. These are often

used for authentication.

**B.** A method for creating similar but inauthentic datasets used for software testing and

user training.

**C.** A method used to protect prying eyes from data such as social security numbers and

credit card data.

**D.** Data masking involves stripping out all similar digits in a string of numbers so as to

obscure the original number.

**6.** Which of the following best describes a sandbox?

**A.** An isolated space where transactions are protected from malicious software

**B.** A space where you can safely execute malicious code to see what it does

**C.** An isolated space where untested code and experimentation can safely occur separate

from the production environment

**D.** An isolated space where untested code and experimentation can safely occur within the

production environment

**7.** Identity and access management (IAM) is a security discipline that ensures which of the

following?

**A.** That all users are properly authorized

**B.** That the right individual gets access to the right resources at the right time for the right

reasons

**C.** That all users are properly authenticated

**D.** That unauthorized users will get access to the right resources at the right time for the

right reasons

**8.** In a federated identity arrangement using a trusted third-party model, who is the identity

provider and who is the relying party?

**A.** A contracted third party/the various member organizations of the federation

**B.** The users of the various organizations within the federation/a CASB

**C.** Each member organization/a trusted third party

**D.** Each member organization/each member organization

**9.** Which of the following best describes the Organizational Normative Framework (ONF)?

**A.** A container for components of an application’s security, best practices, catalogued and

leveraged by the organization

**B.** A framework of containers for all components of application security, best practices,

catalogued and leveraged by the organization

**C.** A set of application security, and best practices, catalogued and leveraged by the organization

**D.** A framework of containers for some of the components of application security, best

practices, catalogued and leveraged by the organization

**10.** APIs are defined as which of the following?

**A.** A set of protocols, and tools for building software applications to access a web-based

software application or tool

**B.** A set of standards for building software applications to access a web-based software

application or tool

**C.** A set of routines, standards, protocols, and tools for building software applications to

access a web-based software application or tool

**D.** A set of routines and tools for building software applications to access web-based

Software applications

**11.** The application normative framework is best described as which of the following?

**A.** A stand-alone framework for storing security practices for the ONF

**B.** A subset of the ONF

**C.** A superset of the ONF

**D.** The complete ONF

**12.** Which of the following best describes SAML?

**A.** A standard for developing secure application management logistics

**B.** A standard for exchanging authentication and authorization data between security

domains

**C.** A standard for exchanging usernames and passwords across devices

**D.** A standard used for directory synchronization

**13.** Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

**A.** Describes international privacy standards for cloud computing

**B.** Provides an overview of application security that introduces definitive concepts, principles,

and processes involved in application security

**C.** Serves as a newer replacement for NIST 800-53 r4

**D.** Provides an overview of network and infrastructure security designed to secure cloud

Applications

**14.** Which of the following best describes data masking?

**A.** Data masking is used in place of encryption for better performance.

**B.** Data masking is used to hide PII.

**C.** Data masking is used to create a similar, inauthentic dataset used for training and

Software testing.

**D.** Data masking is used in place of production data.

**15.** Database activity monitoring (DAM) can be:

**A.** Host-based or network-based

**B.** Server-based or client-based

**C.** Used in the place of encryption

**D.** Used in place of data masking

**16.** Web application firewalls (WAFs) are designed primarily to protect applications from

Common attacks like:

**A.** Syn floods

**B.** Ransomware

**C.** XSS and SQL injection

**D.** Password cracking

**17.** Multifactor authentication consists of at least two items. Which of the following best represents

this concept?

**A.** A complex password and a secret code

**B.** Complex passwords and an HSM

**C.** A hardware token and a magnetic strip card

**D.** Something you know and something you have

**18.** SOAP is a protocol specification providing for the exchange of structured information or

data in web services. Which of the following is *not* true of SOAP?

**A.** Standards-based

**B.** Reliant on XML

**C.** Extremely fast

**D.** Works over numerous protocols

**19.** Dynamic application security testing (DAST) is best described as which of the following?

**A.** Test performed on an application or software product while it is using real data in

production

**B.** Test performed on an application or software product while it is being executed in

memory in an operating system.

**C.** Test performed on an application or software product while being consumed by cloud

customers

**D.** Masking

**20.** Sandboxing provides which of the following?

**A.** A test environment that isolates untrusted code changes for testing in a production

environment

**B.** A test environment that isolates untrusted code changes for testing in a nonproduction

environment

**C.** A testing environment where new and experimental code can be tested in a production

environment

**D.** A testing environment that prevents isolated code from running in a nonproduction

Environment

Chapter 4: Cloud Application Security Answers

**1.** B. The other answers all list aspects of SOAP.

**2.** B. The other answers are all possible stages used in software development.

**3.** D. The other answers all include aspects of the STRIDE model.

**4.** C. All the possible answers are good, and are, in fact, correct. C, however, is the most complete

and therefore the best answer.

**5.** B. Again, all of these answers are actually correct, but B is the best answer, because it is

the most general, includes the others, and is therefore the optimum choice. This is a good

example of the type of question that can appear on the actual exam.

**6.** C. Options A and B are also correct, but C is more general and incorporates them both.

D is incorrect, because sandboxing does not take place in the production environment.

**7.** B. Options A and C are also correct, but included in B, making B the best choice. D is

incorrect, because we don’t want unauthorized users gaining access.

**8.** A. In a trusted third-party model of federation, each member organization outsources the

review and approval task to a third party they all trust. This makes the third party the identifier

(it issues and manages identities for all users in all organizations in the federation),

and the various member organizations are the relying parties (the resource providers that

share resources based on approval from the third party).

**9.** B. Option A is incorrect, because it refers to a specific applications security elements,

meaning it is about an ANF, not the ONF. C is true, but not as complete as B, making B

the better choice. D suggests that the framework contains only “some” of the components,

which is why B (which describes “all” components) is better.

**10.** C. All the answers are true, but C is the most complete.

**11.** B. Remember, there is a one-to-many ratio of ONF to ANF; each organization has one

ONF and many ANFs (one for each application in the organization). Therefore, the ANF is

a subset of the ONF.

**12.** B. Option C is also true, but not as comprehensive as B. A and D are simply not true.

**13.** B. Option B is a description of the standard; the others are not.

**14.** C. Options B and D are also correct, but not as comprehensive as C, making C the best

choice. A is not correct; we don’t want to encrypt data if we’re using the data for testing or

display purposes, the common uses of masked data.

**15.** A. We don’t use DAM in place of encryption or masking; DAM augments these options

without replacing them. We don’t usually think of the database interaction as client-server,

so A is the best answer.

**16.** C. WAFs detect how the application interacts with the environment, so they are optimal for

detecting and refuting things like SQL injection and XSS. Password cracking, syn floods,

and ransomware usually aren’t taking place in the same way as injection and XSS, and they

are better addressed with controls at the router and through the use of HIDS, NIDS, and

antimalware tools.

**17.** D. Option D is the best, most general, and most accurate answer.

**18.** C. The other answers are true of SOAP.

**19.** B. We do the testing prior to deployment, so A and C are incorrect. D is simply a distractor.

**20.** A. Options B and C are incorrect, because a sandbox is not in the production environment.

D is incorrect in that sandboxing does not prevent code from running.